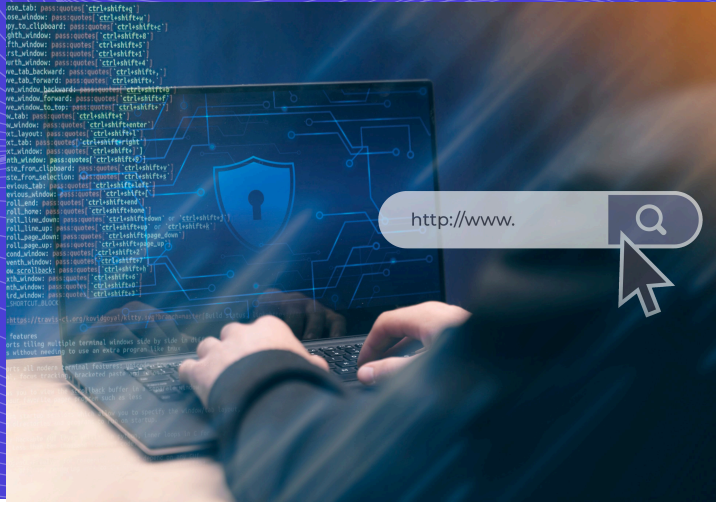
The Beginner's Guide to FINRA Cybersecurity Compliance with Kitecyber

Discover how Kitecyber helps broker-dealers and financial services firms meet FINRA's expectations for cybersecurity, vendor oversight, incident remediation, and protection of customer information.



FINRA / SEC Cyber & Tech Governance Expectations

- Firms must maintain **written policies and procedures** that protect customer data (Rule 30 of SEC Regulation S-P) and manage cybersecurity risk.
- Firms are expected to **supervise and monitor branch offices and vendor relationships** to ensure consistent cybersecurity across the enterprise.
- FINRA emphasizes **incident response readiness**, voluntary reporting, and auditability of cyber events.
- Identity theft prevention (Regulation S-ID / Red Flags) is also a recognized risk when firms manage customer accounts and online access.
- Third-party / vendor risk is increasingly scrutinized — oversight, due diligence, and continuous monitoring of service providers are required.

How Kitecyber Supports FINRA Compliance

Kitecyber's AI Security Copilot, which includes features like DLP, UEM, UEBA, Data Classification, SWG, & ZTNA can help firms meet FINRA's expectations through:

- Preventing leakage or misuse of nonpublic customer or firm data
- Detecting anomalous or insider behavior
- Enforcing strong device posture, least-privilege access, and segmentation
- Monitoring branches and vendor endpoints centrally
- Providing audit trails and incident forensics

FINRA / Cyber Risk Expectations → Kitecyber Mapping Table

FINRA / Cyber Expectation	Mapped Kitecyber Product(s)	How Kitecyber Helps
Written policies, procedures & oversight (Reg S-P, FINRA supervision rules)	DLP, UEM, Compliance Workflows	DLP logs, policy enforcement, access controls; UEM enforces baseline security; workflows automate policy attestation and audit record generation.
Supervision / branch office controls	UEM, DLP, SWG, ZTNA	UEM inventory and posture check of branch devices; DLP monitors data flows; SWG enforces secure web/ SaaS controls; ZTNA segments branch access to core systems.
Vendor / third-party oversight	DLP, UEBA, SWG, ZTNA	DLP monitors data sent to external vendors; UEBA detects anomalous vendor behavior; SWG limits vendor internet/app access; ZTNA enforces secure remote access with minimal privileges.
Incident response readiness & reporting	DLP, UEBA, Audit Logs	DLP captures data exfil events, UEBA correlates suspicious signals, audit logs provide forensic evidence; workflows trigger reporting, containment, and post-mortem.
Identity theft prevention / account security	ZTNA, DLP, UEBA, SWG	ZTNA enforces MFA, device verification, and session policies; DLP scans for leaked credentials; UEBA detects credential misuse; SWG blocks phishing/ imposter sites.
Data protection (customer nonpublic info)	Data Classification, DLP, UEM	Classification identifies sensitive customer data; DLP prevents unauthorized copying or transfer; UEM enforces encryption, disallows insecure storage.
Monitoring, logging, and audit trails	DLP, UEBA, ZTNA, SWG	All modules generate logs of user activity, data access, policy violations, session metadata, which are exportable for regulatory review.
Patch management, secure configuration & system integrity	UEM, UEBA	UEM enforces timely patching, baseline configuration, vulnerability remediation; UEBA flags deviations or suspicious system modifications.
Testing / exercising IRP and recovery	UEBA, DLP, Compliance Workflows	Simulated attack vectors can test DLP / detection effectiveness; UEBA supports rule tuning; compliance workflows enforce review / drills.
Scalability / alignment with firm's risk profile	All modules (configurable)	Kitecyber can scale per branch, region, or business unit; modules tuned per risk, with audit and governance layers.

What Kitecyber Enables for FINRA Compliance

- Reduced risk of customer data breaches — by enforcing endpoint & network DLP.
- Early detection of insider threats — via UEBA and anomaly correlation.
- Secure branch & remote operations — with UEM posture enforcement + ZTNA for access control.
- Vendor oversight — visibility into third-party interactions, controls over data transfers
- Audit-ready evidence — policy logs, incident records, configuration snapshots.
- Incident response orchestration — integrated triggers, reports, containment workflows.

Implementation Roadmap for Broker-Dealers

1. **Inventory data & classify nonpublic customer information** across endpoints, app servers, cloud, and vendor systems.
2. **Deploy DLP policies** to block unauthorized copying, email leaks, or SaaS exfiltration of customer data.
3. **Roll out UEM** baseline (encryption, patching, disable USBs, secure configuration) across branches and remote agents.
4. **Implement ZTNA and SWG** for secure, segmented access to trading, CRM, and back-office systems (minimize exposure).
5. **Enable UEBA & logging** to detect anomalous behavior and produce audit reports to feed to compliance teams / regulators.
6. **Design incident response workflows,** link automated alerts & policy violations to escalation and forensic capture.
7. **Extend oversight to vendors / third parties —** monitor, restrict, and audit their access to your systems/data.
8. **Test and refine** via tabletop exercises, mock intrusion tests, and regular reviews of controls and policies.

KITE CYBER

Kitecyber, 691 S Milpitas Blvd, Ste 217, Milpitas, CA 95035

Email: info@kitecyber.com

Website: www.kitecyber.com

LinkedIn Twitter YouTube